IN THE CLAIMS

Claims 1-5, 7-13, and 15-34 are pending.

Claims 6 and 14 were previously canceled.

Claims 1, 9, 16, 23, 30 and 34 are currently amended.

1. (Currently amended) An out-of-band method for asynchronously establishing a secure association ~~trust relationship~~ with a remote node, comprising:

generating a local public value and a local private value on at least one node;

storing the public value for configuration of the secure association on an out-of-band computer-readable storage medium, wherein the stored public value is not used for authentication;

transporting the out-of-band computer-readable storage medium to the other node;

receiving the public value from the other node via the out-of-band computer-readable storage medium; and

generating a secret value using the local private value in combination with the public value received from the other node; wherein the receiving is asynchronous to the generating.

2. (Original) A method according to Claim 1, wherein the method is performed on both of a pair of nodes, and wherein further the secret values generated at both of the nodes are symmetric.

3. (Original) A method according to Claim 2, wherein the generating a secret value includes performing a Diffie-Hellman computation.

4. (Original) A method according to Claim 1, further comprising:

retaining the secret value locally;

protecting the secret value using the public value received from the other node; and

transmitting the protected secret value to the other node via the out-of-band mechanism.

5. (Original) A method according to Claim 4, wherein the generating a secret value includes performing a Rivest-Shamir-Adleman (RSA) computation.

6. (Canceled)

7. (Original) A method according to Claim 1, wherein the receiving of the public value from the other node via an out-of-band mechanism includes downloading the public value from an external device.

8. (Original) A method according to Claim 7, wherein the external device is any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

9. (Currently amended) A computer-readable storage medium having one or more instructions causing one or more processors to:

generate a local two-part code having a public code component and private code component;

store the public component on a peripheral out-of-band device which is then transported to a another processor for configuration of the secure association and not authentication;

receive the public code component asynchronously from another processor via the peripheral device; and

generate a secret value using the local private code component and the public code component received from the other processor.

10. (Previously amended) A computer-readable storage medium according to Claim 9, wherein the one or more instructions are executed on the other processor, and wherein further the secret value is symmetrical to the secret value generated on the other processor.

11. (Previously amended) A computer-readable storage medium according to Claim 9, wherein the one or more instructions to generate a secret value includes one or more instructions to perform a Diffie-Hellman computation.

12. (Previously amended) A computer-readable storage medium according to Claim 9, further comprising one or more instructions causing one or more processors to:

encode the secret value using the public code component received from the other processor; and

transmit the encoded secret value to the other processor via the peripheral device.

13. (Previously amended) A computer-readable storage medium according to Claim 12, wherein the one or more instructions to generate a secret value includes one or more instructions to perform an RSA computation.

14. (Canceled)

15. (Previously amended) A computer-readable storage medium according to Claim 9, wherein the one or more instructions to receive the public code component from the other processor via the peripheral device includes downloading the public code component from one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

16. (Currently amended) An apparatus, comprising:

a computer-readable storage medium;

a key generator on a first node to generate a local public/private key pair;

a computer processor executing code to write ~~capable of writing~~ the local public/private key pair to an out-of-band computer-readable storage medium to facilitate setup of a secure association and not for authentication;

~~a method of transporting the out-of-band computer-readable storage medium to a second node;~~ and

a shared secret generator on the second node to receive the public key from the first node via the out-of-band computer-readable storage medium connection and which is able to generate a shared secret using the local private key and the public key received from the first node.

17. (Original) An apparatus according to Claim 16, wherein the shared secret is symmetrical to a shared secret generated on the other node using the local public key and a private key corresponding to the other node.

18. (Original) An apparatus according to Claim 16, wherein the other node is a server.

19. (Original) An apparatus according to Claim 16, wherein the shared secret generator is to generate a shared secret by performing a Diffie-Hellman computation.

20. (Original) An apparatus according to Claim 16, further comprising an encoder to encode the secret value using the public key received from the other node and to transmit the encoded secret value to the other node via the out-of-band connection.

21. (Original) An apparatus according to Claim 20, wherein the shared secret generator is to generate a shared secret by performing an RSA computation.

22. (Original) An apparatus according to Claim 16, wherein the out-of-band connection includes any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

23. (Currently amended) A protocol for establishing a trust relationship between two or more processing nodes, comprising:

generating a public key and a private key on each of at least two nodes;

exchanging the public keys asynchronously between the at least two nodes

using an out-of-band mechanism comprising a computer-readable storage medium wherein the public keys are not used for authentication; and

calculating a secret to be shared on at least one of the two nodes.

24. (Original) A protocol according to Claim 23, wherein the calculating of the secret to be shared includes performing a function using the public key from the other of the two nodes and the private key.

25. (Original) A protocol according to Claim 24, wherein the calculating the secret to be shared includes performing a Diffie-Hellman calculation.

26. (Original) A protocol according to Claim 24, wherein the secret to be shared is symmetrical on the at least two nodes.

27. (Previously amended) A protocol according to Claim 23, further comprising:

encoding the secret to be shared using the public key from the other of the two nodes; and

transmitting the encoded secret to be shared to the other of the two nodes via the out-of-band mechanism.

28. (Original) A protocol according to Claim 27, wherein the calculating the secret to be shared includes performing an RSA calculation.

29. (Original) A protocol according to Claim 23, wherein the out-of-band mechanism includes any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.

30. (Currently amended) An apparatus, comprising:

means for generating a local public/private key pair;

means for storing a public key on an out-of-band computer-readable storage medium;

means for transporting asynchronously the public key to another node;

means for receiving at another node the public key from the out-of-band computer-readable storage medium wherein the public key is not used for authentication; and

means for generating a shared secret using the local private key and the public key received from the other node asynchronously via the out-of-band computer-readable storage medium.

31. (Original) An apparatus according to Claim 30, wherein the means for generating a shared secret performs a Diffie-Hellman computation.

32. (Original) An apparatus according to Claim 30, further comprising means for encoding the shared secret using the public key received from the other node.

33. (Original) An apparatus according to Claim 32, wherein the means for generating a shared secret performs an RSA computation.

34. (Currently amended) An apparatus according to Claim 30, wherein the out-of-band computer-readable storage medium includes any one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible device.